

ONE HUNDRED THIRTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

October 30, 2014

The Honorable Gene Dodaro
Comptroller General
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20248

Dear Mr. Dodaro:

The Federal Information Security Management Act of 2002 (FISMA) requires that each federal agency designate a “senior agency information security officer” whose primary responsibilities are the “development and maintenance of information security policies, procedures and control techniques.”¹ Commonly known as Chief Information Security Officers (CISOs), these officials oversee the security of their agency’s data, networks, and information, including those provided and maintained by agency contractors. Yet, the federal government continues to suffer frequent cyber breaches.

According to the FY 2013 FISMA report, agencies reported over 227,992 security incidents to the United States Computer Emergency Readiness Team (US-CERT)². During that same time period, those agencies spent a total of \$10.3 billion in support of information security efforts.³ Robert Anderson, the Executive Assistant Director of the Criminal, Cyber, Response, and Services Branch at the FBI, told senators at a recent hearing that he believes that every major federal department has been hacked.⁴ Taking into account the statutory authority provided by FISMA and the monetary resources allocated for information security, we are concerned by federal agencies inability to adequately protect their data, networks, and information.

Given the sensitivity, importance, and amount of data for which the federal government is responsible, we ask that the Government Accountability Office (GAO) conduct a government-

¹ Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3544(a)(3) (2002).

² Office of Management and Budget, Annual Report to Congress: Federal Information Security Management Act 33 (2014).

³ *Id.* at 59.

⁴ *Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs, 113th Cong. (2014)* (statement of Robert Anderson, Executive Assistant Director, Criminal, Cyber, Response, and Services Branch, Federal Bureau of Investigation).

wide survey of current CISO authorities. In particular, we request that GAO investigate the following items:

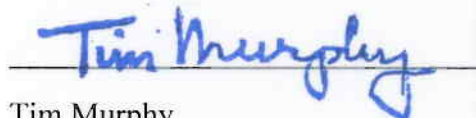
1. What policies, procedures, or authorities has each agency enacted in order to satisfy the referenced FISMA requirement?
2. Where in the organizational hierarchy of each agency is the office of the CISO located?
3. What authority does each office of the CISO have over information technology procurement and maintenance?
4. What authority does each office of the CISO have over operational decisions?
5. What authority does each office of the CISO have over contractor owned and operated portions of the agency's network?
6. What procedures and practices should be uniform throughout the government for a CISO?
7. What procedures and practices adopted by some CISOs but not all should be strongly encouraged throughout the government if not outright required?
8. What procedures and practices adopted by some CISOs but not others should be discouraged or prohibited?

If you have any questions regarding this request, please contact Sean Hayes or Jessica Wilkerson with the Committee staff at (202) 225-2927.

Sincerely,



Fred Upton
Chairman



Tim Murphy
Chairman
Subcommittee on Oversight and Investigations